

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-259106

(43)Date of publication of application : 16.09.2004

(51)Int.Cl.

G06F 9/46

(21)Application number : 2003-050701

(71)Applicant : NTT DATA CORP

(22)Date of filing : 27.02.2003

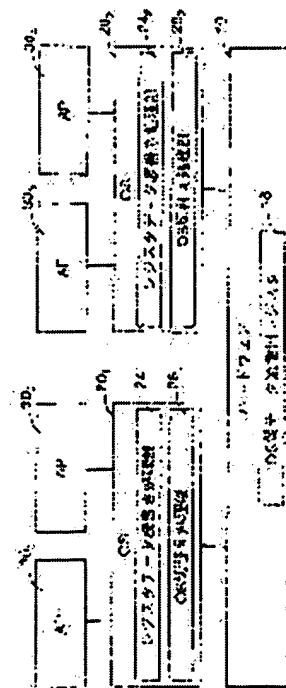
(72)Inventor : TANIGUCHI HIDEO
NOMURA YOSHINARI
TANAKA KAZUO
ITO KENICHI
NAKAJIMA YUSAKU
TABUCHI MASAKI
MASUMOTO KEI

(54) MULTI-OPERATING SYSTEM CONTROL METHOD, PROGRAM FOR MAKING COMPUTER PERFORM METHOD, AND MULTI-OPERATING SYSTEM CONTROL DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a multi-operating system control method capable of improving the security and reliability of a multi-operating system, and provide a program for making a computer perform the method and a multi-operating system control device.

SOLUTION: In the case of transmitting data from OS201 to OS202, a register data read/write processing part 24 of OS201 writes transmit data in OS-to-OS data communication register 18. After switching from OS201 to OS202 is performed by an OS switching processing part 281, a register data read/write processing part 242 of the OS202 reads out data from the OS-to-OS data communication register 18.



LEGAL STATUS

[Date of request for examination] 27.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-259106

(P2004-259106A)

(43) 公開日 平成16年9月16日 (2004. 9. 16)

(51) Int.Cl.⁷
G06F 9/46F I
G06F 9/46 350テーマコード (参考)
5B098

審査請求 有 請求項の数 11 O L (全 34 頁)

(21) 出願番号 特願2003-50701 (P2003-50701)
(22) 出願日 平成15年2月27日 (2003. 2. 27)(71) 出願人 000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(74) 代理人 100089118
弁理士 酒井 宏明
(72) 発明者 谷口 秀夫
福岡県福岡市東区箱崎6丁目10番1号
九州大学大学院内
(72) 発明者 乃村 能成
福岡県福岡市東区箱崎6丁目10番1号
九州大学大学院内
(72) 発明者 田中 一男
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

最終頁に続く

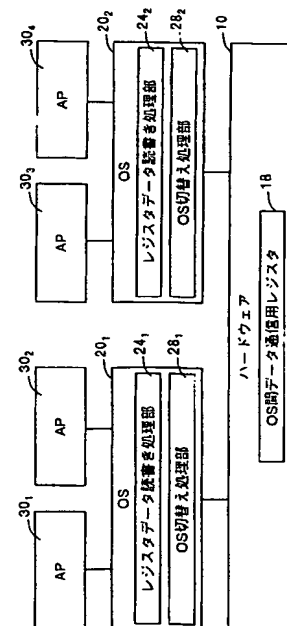
(54) 【発明の名称】 マルチオペレーティングシステム制御方法、およびその方法をコンピュータに実行させるプログラム、ならびにマルチオペレーティングシステム制御装置

(57) 【要約】

【課題】 マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができるマルチオペレーティングシステム制御方法、およびその方法をコンピュータに実行させるプログラム、ならびにマルチオペレーティングシステム制御装置を提供すること。

【解決手段】 OS 20₁ から OS 20₂ へデータを送信する場合に、OS 20₁ のレジスタデータ読書き処理部 24₁ が OS 間データ通信用レジスタ 18 に送信するデータを書き込み、OS 切り替え処理部 28₁ により、OS 20₁ から OS 20₂ への切り替えが実行された後、OS 20₂ のレジスタデータ読書き処理部 24₂ が OS 間データ通信用レジスタ 18 からデータを読み出す。

【選択図】 図 1



【特許請求の範囲】

【請求項 1】

一つの計算機で稼動する第 1 のオペレーティングシステムおよび第 2 のオペレーティングシステムを切り替え制御するマルチオペレーティングシステム制御方法であって、前記第 1 のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納するデータ格納工程と、前記第 1 のオペレーティングシステムから前記第 2 のオペレーティングシステムに切り替えがなされた場合に、前記所定のレジスタから前記通信対象となるデータを取得するデータ取得工程と、を含んだことを特徴とするマルチオペレーティングシステム制御方法。

10

【請求項 2】

前記データ格納工程により前記所定のレジスタに通信対象となるデータが格納された際に、前記第 1 のオペレーティングシステムに対応する第 1 の仮想メモリ空間の論理アドレス N にあらかじめ仮想記憶された、前記第 1 のオペレーティングシステムから前記第 2 のオペレーティングシステムへ切り替える第 1 の切り替え命令により、前記第 1 のオペレーティングシステムから前記第 2 のオペレーティングシステムに切り替え、前記データ取得工程により、前記第 2 のオペレーティングシステムに対応する第 2 の仮想メモリ空間の論理アドレス N + 1 にあらかじめ記憶されたデータ取得命令、または、該論理アドレス N + 1 にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、前記所定のレジスタから前記通信対象となるデータを取得することを特徴とする請求項 1 に記載のマルチオペレーティングシステム制御方法。

20

【請求項 3】

前記第 2 のオペレーティングシステムは、前記データ取得命令を実行した後、あらかじめ仮想記憶された前記第 2 のオペレーティングシステムから前記第 1 のオペレーティングシステムへ切り替えるための第 2 の切り替え命令により、前記第 2 のオペレーティングシステムから前記第 1 のオペレーティングシステムに切り替えることを特徴とする請求項 2 に記載のマルチオペレーティングシステム制御方法。

【請求項 4】

所定のレジスタに格納されているデータをバックアップするデータバックアップ工程と、バックアップされた前記データを該データが格納されていた前記所定のレジスタに復元するデータ復元工程とをさらに含み、前記データ格納工程では、前記データバックアップ工程によりデータがバックアップされたレジスタに通信対象となるデータを格納し、前記第 2 の切り替え命令により、前記第 2 のオペレーティングシステムから前記第 1 のオペレーティングシステムに切り替えがおこなわれた際に、前記データ復元工程により、バックアップされた前記データを該データが格納されていた前記所定のレジスタに復元することを特徴とする請求項 3 に記載のマルチオペレーティングシステム制御方法。

30

【請求項 5】

前記所定のレジスタは、前記第 1 のオペレーティングシステムの実行中に第 1 のオペレーティングシステムにより使用されていないレジスタであることを特徴とする請求項 1 ~ 4 のいずれか一つに記載のマルチオペレーティングシステム制御方法。

40

【請求項 6】

前記所定のレジスタは、前記第 1 のオペレーティングシステムの実行中に第 1 のオペレーティングシステムにより使用されていないデバッグレジスタおよび／または汎用レジスタであることを特徴とする請求項 5 に記載のマルチオペレーティングシステム制御方法。

【請求項 7】

前記データ格納工程は、前記通信対象となるデータのサイズが前記所定のレジスタに格納できるサイズかどうかを判定するデータサイズ判定工程をさらに含み、格納できる場合には該所定のレジスタにデータを格納し、格納できない場合には、前記所定のレジスタ以外の格納手段により前記通信対象となるデータを格納し、格納されたデータを前記第 2 のオペレーティングシステムが取得することを特徴とする請求項 1 ~ 6 のいずれか一つに記載

50

のマルチオペレーティングシステム制御方法。

【請求項 8】

前記格納手段は、ネットワークインターフェースカードに備えられた格納手段であり、前記第 2 のオペレーティングシステム宛の前記通信対象となるデータが該格納手段に格納された場合に、該格納手段の接続を、前記第 1 のオペレーティングシステムを中継して前記第 2 のオペレーティングシステムに設定することを特徴とする請求項 7 に記載のマルチオペレーティングシステム制御方法。

【請求項 9】

請求項 1 ～ 8 のいずれか一つに記載されたマルチオペレーティングシステム制御方法をコンピュータに実行させるプログラム。

10

【請求項 10】

一つの計算機で稼動する第 1 のオペレーティングシステムおよび第 2 のオペレーティングシステムを切り替え制御するマルチオペレーティングシステム制御装置であって、前記第 1 のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納するデータ格納手段と、

前記第 1 のオペレーティングシステムから前記第 2 のオペレーティングシステムに切り替えがなされた場合に、前記所定のレジスタから前記通信対象となるデータを取得するデータ取得手段と、

を備えたことを特徴とするマルチオペレーティングシステム制御装置。

【請求項 11】

20

前記データ格納手段により前記所定のレジスタに通信対象となるデータが格納された際に、前記第 1 のオペレーティングシステムに対応する第 1 の仮想メモリ空間の論理アドレス N にあらかじめ仮想記憶された、前記第 1 のオペレーティングシステムから前記第 2 のオペレーティングシステムへ切り替える第 1 の切り替え命令により、前記第 1 のオペレーティングシステムから前記第 2 のオペレーティングシステムに切り替え、前記データ取得手段は、前記第 2 のオペレーティングシステムに対応する第 2 の仮想メモリ空間の論理アドレス N + 1 にあらかじめ記憶されたデータ取得命令、または、該論理アドレス N + 1 にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、前記所定のレジスタから前記通信対象となるデータを取得することを特徴とする請求項 10 に記載のマルチオペレーティングシステム制御装置。

30

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、一台の計算機上で稼動する複数のオペレーティングシステムを切り替え制御するためのマルチオペレーティングシステム制御方法、およびその方法をコンピュータに実行させるプログラム、ならびにマルチオペレーティングシステム制御装置に関するものであり、特に、セキュリティ、信頼性を向上させることができるマルチオペレーティングシステム制御方法、およびその方法をコンピュータに実行させるプログラム、ならびにオペレーティングシステム制御装置に関するものである。

【0002】

40

【従来の技術】

通常の計算機では、1つのオペレーティングシステムが動作し、それが計算機のプロセッサ、メモリ、二次記憶装置等の計算機資源を管理し、計算機が効率良く動作できるように資源スケジュールを実施している。オペレーティングシステムには、様々な種類がある。バッチ処理に優れるものや、TSS (Time Sharing System) に優れるもの、GUI (Graphical User Interface) に優れているものなど様々である。

【0003】

一方で、これら複数あるオペレーティングシステムを1台の計算機で同時に実行したいというニーズがある。例えば、大型計算機においては、実際の業務に伴うオンライン処理を

50

実行するオペレーティングシステムと、開発用のオペレーティングシステムとを一台の計算機で動作させたいという要求がある。あるいは、GUIの整っているオペレーティングシステムと、実時間性に優れているオペレーティングシステムとを同時に稼働させたい等という要求もある。

【0004】

しかしながら、個々のオペレーティングシステムは、単独で計算機資源の管理を実施することを前提として設計されている。従って、複数のオペレーティングシステムの共存は、何らかの機構なしには不可能である。

【0005】

一台の計算機上で複数のオペレーティングシステムを動作させる機構としては、大型計算機で実現されている仮想計算機方式がある。図21は、上記仮想計算機方式による従来のマルチオペレーティングシステムの構成例1を示すブロック図である。

10

【0006】

同図に示したマルチオペレーティングシステムは、ハードウェア1、基盤OS2、VM (Virtual Machine) モニタ3、仮想OS (オペレーティングシステム) 4₁、仮想OS 4₂ および仮想OS 4₃ から構成されている。

【0007】

ハードウェア1は、CPU (Central Processing Unit)、物理メモリ、入出力機器等である。基盤OS2およびVMモニタ3は、ハードウェア1の全てを制御している。VMモニタ3は、仮想OS 4₁ ~ 4₃ のそれぞれのハードウェア1に対するインタフェースをエミュレートする。仮想OS 4₁ ~ 4₃ は、基盤OS2の上で走行する。すなわち、基盤OS2と仮想OS 4₁ ~ 4₃ とは、主従関係にある。

20

【0008】

同図に示したマルチオペレーティングシステムにおいて、例えば、仮想OS間でデータの通信を行う場合、基盤OS2や、仮想OS 4₁ ~ 4₃ から同時に参照可能な共有メモリ (図示略) を経由する方法が採られる。

【0009】

例えば、仮想OS 4₁ から仮想OS 4₂ へデータを送信する場合には、仮想OS 4₁ がデータを共有メモリに格納した後、仮想OS 4₂ が共有メモリからデータを取得する。なお、仮想OS間以外に、仮想OSと他装置との間においても、共有メモリや基盤OS2を経由して通信が行われる。

30

【0010】

また、一台の計算機で複数のオペレーティングシステムのインタフェースを提供する技術として、マイクロカーネル方式がある。図22は、上記マイクロカーネル方式による従来のマルチオペレーティングシステムの構成例2を示すブロック図である。

【0011】

同図に示したマルチオペレーティングシステムは、ハードウェア5、マイクロカーネル (制御プログラム) 6、OS 7₁、OS 7₂ およびOS 7₃ から構成されている。

【0012】

マイクロカーネル方式では、マイクロカーネル6の上に、ユーザに見せるオペレーティングシステム機能を提供するOS 7₁ ~ 7₃ が構築されている。ユーザはOS 7₁ ~ 7₃ を経由してハードウェア5 (計算機資源) を利用する。マイクロカーネル6は、OS 7₁ ~ 7₃ を制御する。

40

【0013】

同図に示したマルチオペレーティングシステムにおいて、例えば、OS間でデータの通信を行う場合にも、マイクロカーネルや、OS 7₁ ~ 7₃ から同時に参照可能な共有メモリ (図示略) を経由する方法が採られる。

【0014】

例えば、OS 7₁ からOS 7₂ へデータを送信する場合には、OS 7₁ がデータを共有メモリに格納した後、OS 7₂ が共有メモリからデータを取得する。なお、OS間

50

以外に、OSと他装置との間においても、共有メモリやマイクロカーネル6を経由して通信が行われる。

【0015】

【特許文献1】

特開平11-149385号公報

【特許文献2】

特開2001-216172号公報

【特許文献3】

特開2000-207232号公報

【特許文献4】

特開平8-212089号公報

【特許文献5】

特開2001-290661号公報

【特許文献6】

特開平11-85546号公報

【特許文献7】

特開2001-282558号公報

【特許文献8】

特開平11-85546号公報

【0016】

【発明が解決しようとする課題】

ところで、前述したように、図21に示した従来のマルチオペレーティングシステムにおいては、仮想OS間や仮想OSと他装置との間で共用メモリを経由して通信を行っているため、セキュリティが低いという問題があった。

【0017】

すなわち、上記共用メモリが複数の仮想OS $4_1 \sim 4_3$ のそれぞれから同時に参照可能であるため、通信時に共用メモリに外部から不正アクセスされた場合には、仮想OS $4_1 \sim 4_3$ が同時に攻撃される。

【0018】

また、図22に示した従来のマルチオペレーティングシステムにおいても、共用メモリが複数のOS $7_1 \sim 7_3$ のそれぞれから同時に参照可能であるため、通信時に共用メモリに外部から不正アクセスされた場合に、OS $7_1 \sim 7_3$ が同時に攻撃され、セキュリティ上問題がある。

【0019】

本発明は、上記に鑑みてなされたものであり、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができるマルチオペレーティングシステム制御方法、およびその方法をコンピュータに実行させるプログラム、ならびにマルチオペレーティングシステム制御装置を提供することを目的とする。

【0020】

【課題を解決するための手段】

上記目的を達成するために、本発明に係るマルチオペレーティングシステム制御方法にあつては、一つの計算機で稼動する第1のオペレーティングシステムおよび第2のオペレーティングシステムを切り替え制御するマルチオペレーティングシステム制御方法であつて、前記第1のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納するデータ格納工程と、前記第1のオペレーティングシステムから前記第2のオペレーティングシステムに切り替えがなされた場合に、前記所定のレジスタから前記通信対象となるデータを取得するデータ取得工程と、を含んだことを特徴とする。

【0021】

この発明によれば、第1のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納し、第1のオペレーティングシステムから第2のオペレーティング

10

20

30

40

50

システムに切り替えがなされた場合に、所定のレジスタから通信対象となるデータを取得することとしたので、共有メモリを介さずに、格納できるデータのサイズが制限されたレジスタをオペレーティングシステム間の通信に用いることで、不正なデータの通信による各オペレーティングシステムの異常動作の可能性を回避することができ、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0022】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、前記データ格納工程により前記所定のレジスタに通信対象となるデータが格納された際に、前記第1のオペレーティングシステムに対応する第1の仮想メモリ空間の論理アドレスNにあらかじめ仮想記憶された、前記第1のオペレーティングシステムから前記第2のオペレーティングシステムへ切り替える第1の切り替え命令により、前記第1のオペレーティングシステムから前記第2のオペレーティングシステムに切り替え、前記データ取得工程により、前記第2のオペレーティングシステムに対応する第2の仮想メモリ空間の論理アドレスN+1にあらかじめ記憶されたデータ取得命令、または、該論理アドレスN+1にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、前記所定のレジスタから前記通信対象となるデータを取得することを特徴とする。

【0023】

この発明によれば、所定のレジスタに通信対象となるデータが格納された際に、第1のオペレーティングシステムに対応する第1の仮想メモリ空間の論理アドレスNにあらかじめ仮想記憶された、第1のオペレーティングシステムから第2のオペレーティングシステムへ切り替える第1の切り替え命令により、第1のオペレーティングシステムから第2のオペレーティングシステムに切り替え、第2のオペレーティングシステムに対応する第2の仮想メモリ空間の論理アドレスN+1にあらかじめ記憶されたデータ取得命令、または、該論理アドレスN+1にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、所定のレジスタから通信対象となるデータを取得することとしたので、従来の基盤OSやVMモニタ等の共通部分が不要で、第1および第2のオペレーティングシステムが共存され、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0024】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、前記第2のオペレーティングシステムは、前記データ取得命令を実行した後、あらかじめ仮想記憶された前記第2のオペレーティングシステムから前記第1のオペレーティングシステムへ切り替えるための第2の切り替え命令により、前記第2のオペレーティングシステムから前記第1のオペレーティングシステムに切り替えることを特徴とする。

【0025】

この発明によれば、第2のオペレーティングシステムは、データ取得命令を実行した後、あらかじめ仮想記憶された第2のオペレーティングシステムから第1のオペレーティングシステムへ切り替えるための第2の切り替え命令により、第2のオペレーティングシステムから第1のオペレーティングシステムに切り替えることとしたので、高いセキュリティと信頼性を維持したまま、オペレーティングシステムの切り替えおよび切り戻しを円滑におこなうことができる。

【0026】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、所定のレジスタに格納されているデータをバックアップするデータバックアップ工程と、バックアップされた前記データを該データが格納されていた前記所定のレジスタに復元するデータ復元工程とをさらに含み、前記データ格納工程では、前記データバックアップ工程によりデータがバックアップされたレジスタに通信対象となるデータを格納し、前記第2の切り替え命令により、前記第2のオペレーティングシステムから前記第1のオペレーティングシステムに切り替えがおこなわれた際に、前記データ復元工程により、バックアップされた前記データを該データが格納されていた前記所定のレジスタに復元することを特徴とする。

【0027】

この発明によれば、所定のレジスタに格納されているデータをバックアップし、データがバックアップされたレジスタに通信対象となるデータを格納し、第2の切り替え命令により、第2のオペレーティングシステムから第1のオペレーティングシステムに切り替えがおこなわれた際に、バックアップされたデータをデータが格納されていた所定のレジスタに復元することとしたので、第1のオペレーティングシステムの実行中に使用されているレジスタにオペレーティングシステム間で通信するデータを格納することができ、そのレジスタを利用して通信をおこなうことにより、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0028】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、前記所定のレジスタは、前記第1のオペレーティングシステムの実行中に第1のオペレーティングシステムにより使用されていないレジスタであることを特徴とする。

10

【0029】

この発明によれば、所定のレジスタは、第1のオペレーティングシステムの実行中に第1のオペレーティングシステムにより使用されていないレジスタであることとしたので、オペレーティングシステム間で通信するデータを格納することができ、そのレジスタを利用して通信をおこなうことにより、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0030】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、前記所定のレジスタは、前記第1のオペレーティングシステムの実行中に第1のオペレーティングシステムにより使用されていないデバッグレジスタおよび／または汎用レジスタであることを特徴とする。

20

【0031】

この発明によれば、所定のレジスタは、第1のオペレーティングシステムの実行中に第1のオペレーティングシステムにより使用されていないデバッグレジスタおよび／または汎用レジスタであることとしたので、デバッグレジスタおよび／または汎用レジスタにオペレーティングシステム間で通信するデータを格納することができ、そのレジスタを利用して通信をおこなうことにより、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

30

【0032】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、前記データ格納工程は、前記通信対象となるデータのサイズが前記所定のレジスタに格納できるサイズかどうかを判定するデータサイズ判定工程をさらに含み、格納できる場合には該所定のレジスタにデータを格納し、格納できない場合には、前記所定のレジスタ以外の格納手段により前記通信対象となるデータを格納し、格納されたデータを前記第2のオペレーティングシステムが取得することを特徴とする。

【0033】

この発明によれば、通信対象となるデータのサイズが所定のレジスタに格納できるサイズかどうかを判定し、格納できる場合には所定のレジスタにデータを格納し、格納できない場合には、所定のレジスタ以外の格納手段により通信対象となるデータを格納し、格納されたデータを第2のオペレーティングシステムが取得することとしたので、データのサイズに応じて適切な格納手段を選択することができ、高いセキュリティおよび信頼性を有する効率的なオペレーティングシステム間のデータの通信をおこなうことができる。

40

【0034】

つぎの発明に係るマルチオペレーティングシステム制御方法にあつては、前記格納手段は、ネットワークインターフェースカードに備えられたものであり、前記第2のオペレーティングシステム宛の前記通信対象となるデータが該格納手段に格納された場合に、該格納手段の接続を、前記第1のオペレーティングシステムを中継して前記第2のオペレーティ

50

ングシステムに設定することを特徴とする。

【0035】

この発明によれば、ネットワークインターフェースカードに備えられた格納手段に第2のオペレーティングシステム宛の前記通信対象となるデータが格納された場合に、格納手段の接続を、第1のオペレーティングシステムを中継して第2のオペレーティングシステムに設定することとしたので、通信対象となるデータのサイズが所定のレジスタに格納できないサイズであっても、高いセキュリティおよび信頼性を有する効率的なオペレーティングシステム間のデータの通信をおこなうことができる。

【0036】

つぎの発明に係るプログラムは、上記発明のいずれか一つに記載されたマルチオペレーティングシステム制御方法をコンピュータに実行させるプログラムであり、そのプログラムがコンピュータ読み取り可能となり、これによって、上記発明のいずれか一つの動作をコンピュータによって実行することができる。

【0037】

つぎの発明に係るマルチオペレーティングシステム制御装置にあつては、一つの計算機で稼動する第1のオペレーティングシステムおよび第2のオペレーティングシステムを切り替え制御するマルチオペレーティングシステム制御装置であつて、前記第1のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納するデータ格納手段と、前記第1のオペレーティングシステムから前記第2のオペレーティングシステムに切り替えがなされた場合に、前記所定のレジスタから前記通信対象となるデータを取得するデータ取得手段と、を備えたことを特徴とする。

【0038】

この発明によれば、第1のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納し、第1のオペレーティングシステムから第2のオペレーティングシステムに切り替えがなされた場合に、所定のレジスタから通信対象となるデータを取得することとしたので、共有メモリを介さずに、格納できるデータのサイズが制限されたレジスタをオペレーティングシステム間の通信に用いることで、不正なデータの通信による各オペレーティングシステムの異常動作の可能性を回避することができ、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0039】

つぎの発明に係るマルチオペレーティングシステム制御装置にあつては、前記データ格納手段により前記所定のレジスタに通信対象となるデータが格納された際に、前記第1のオペレーティングシステムに対応する第1の仮想メモリ空間の論理アドレスNにあらかじめ仮想記憶された、前記第1のオペレーティングシステムから前記第2のオペレーティングシステムへ切り替える第1の切り替え命令により、前記第1のオペレーティングシステムから前記第2のオペレーティングシステムに切り替え、前記データ取得手段は、前記第2のオペレーティングシステムに対応する第2の仮想メモリ空間の論理アドレスN+1にあらかじめ記憶されたデータ取得命令、または、該論理アドレスN+1にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、前記所定のレジスタから前記通信対象となるデータを取得することを特徴とする。

【0040】

この発明によれば、所定のレジスタに通信対象となるデータが格納された際に、第1のオペレーティングシステムに対応する第1の仮想メモリ空間の論理アドレスNにあらかじめ仮想記憶された、第1のオペレーティングシステムから第2のオペレーティングシステムへ切り替える第1の切り替え命令により、第1のオペレーティングシステムから第2のオペレーティングシステムに切り替え、第2のオペレーティングシステムに対応する第2の仮想メモリ空間の論理アドレスN+1にあらかじめ記憶されたデータ取得命令、または、該論理アドレスN+1にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、所定のレジスタから通信対象となるデータを取得することとしたので、従来の基盤OSやVMモニタ等の共通部分が不要で、第1および第2のオペレーティングシステム

10

20

30

40

50

が共存され、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0041】

【発明の実施の形態】

以下、図面を参照して本発明にかかるマルチオペレーティングシステム制御方法、およびその方法をコンピュータに実行させるプログラム、ならびにマルチオペレーティングシステム制御装置の実施の形態1および2について詳細に説明する。

【0042】

(実施の形態1)

図1は、本発明に係る実施の形態1の概略構成を示すブロック図である。この図に示したマルチオペレーティングシステムは、ハードウェア10、OS20₁、OS20₂およびAP(アプリケーションプログラム)30₁〜30₄から構成されている。

10

【0043】

また、OS20₁およびOS20₂は、レジスタデータ読書き処理部24₁および24₂、OS切替え処理部28₁および28₂をそれぞれ有する。そして、ハードウェア10は、OS間データ通信用レジスタ18を有する。

【0044】

OS間データ通信用レジスタ18は、OS20₁からOS20₂へ、またはOS20₂からOS20₁へデータを通信する際に、通信するデータを格納するレジスタであり、実行中のOS20₁またはOS20₂により使用されていないレジスタである。通信するデータには、送信先のOSに対するコマンド等も含まれる。

20

【0045】

例えば、インテル社製ペンティアム(登録商標)プロセッサのデバッグレジスタは、デバッグモード時以外では使用されていないレジスタであり、OS間データ通信用レジスタ18として利用できる。

【0046】

同じくインテル社製ペンティアム(登録商標)プロセッサの汎用レジスタECXは、ループの回数をカウントするために用いられるが、ループ処理をおこなっていない場合には使用されておらず、OS間データ通信用レジスタ18として利用できる。

30

【0047】

OS間データ通信用レジスタ18として利用することができるレジスタは、上記のレジスタに限定されず、実行中のOS20₁またはOS20₂により使用されていないレジスタであればよい。

40

【0048】

また、実行中のOS20₁またはOS20₂により使用されているレジスタであっても、レジスタに格納されているデータをメモリなどにバックアップすれば、そのレジスタをOS間データ通信用レジスタ18として利用することができる。

【0049】

ただしこの場合は、データの通信終了後、バックアップされたデータをレジスタに復元する。このようにすることで、データ通信をおこなう以前の状態と同様に、データの通信終了後のレジスタへのアクセスを正常におこなうことができるようになる。

40

【0050】

同マルチオペレーティングシステムでは、OS20₁からOS20₂へ、またはOS20₂からOS20₁への切り替えがOS切替え処理部28₁および28₂によりそれぞれ実行される。割り込みの発生要因としては、OS間データ通信用レジスタ18を介してのデータの通信要求、タイマ(図示略)による定期的な切り替え要求等が挙げられる。

【0051】

データの通信要求による割り込みが発生し、OS20₁からOS20₂へデータを送信する場合には、OS20₁のレジスタデータ読書き処理部24₁によりOS間デー

50

タ通信レジスタ18に送信するデータが書き込まれる（格納される）。

【0052】

そして、OS切替え処理部28₁により、OS20₁からOS20₂への切り替えが実行された後、OS20₂のレジスタデータ読書き処理部24₂によりOS間データ通信レジスタ18からデータが読み出されて（取得されて）、OS間のデータ通信が完了する。

【0053】

OS20₂からOS20₁へデータを送信する場合には、OS20₂のレジスタデータ読書き処理部24₂によりOS間データ通信レジスタ18に送信するデータが書き込まれる。そして、OS切替え処理部28₂により、OS20₂からOS20₁への切り替えが実行された後、OS20₁のレジスタデータ読書き処理部24₁によりOS間データ通信レジスタ18からデータが読み出される。

10

【0054】

ここで、OS間データ通信レジスタ18のサイズは16ビット～80ビット程度と限定されているので、不正なデータやウィルスプログラムがOS20₁とOS20₂との間で伝播しにくく、OSのセキュリティおよび信頼性を向上させることができる。

【0055】

このように、同マルチオペレーティングシステムは、従来のように共通の制御プログラムや、共用メモリ等を介さずに、OS間データ通信レジスタ18を用いて、高いセキュリティを保持した状態でOS20₁とOS20₂との間でデータの受け渡しを実現する

20

【0056】

図2は、実施の形態1の具体的構成を示すブロック図である。この図において、図1の各部に対応する部分には同一の符号を付ける。また、本実施の形態1では、OS間データ通信レジスタ18として、インテル社製ペンティアム（登録商標）プロセッサのデバッグレジスタ15を用いた場合について説明する。

【0057】

図2において、ハードウェア10は、計算機資源であり、制御部11、物理メモリ12、割り込みベクタテーブルレジスタ13、ページテーブルレジスタ14、デバッグレジスタ15、その他のレジスタ16、プログラムカウンタ17や、図示しないキーボード、ディスプレイ等から構成されている。

30

【0058】

ハードウェア10には、マルチ構成のOS20₁およびOS20₂が存在している。OS20₁およびOS20₂のそれぞれは、ハードウェア10の計算機資源を管理し、割り込み処理ルーチンの中で切り替えられる。すなわち、ある時間を考えると、ハードウェア10は、一つのOS（OS20₁またはOS20₂）により占有される。

【0059】

OS20₁は、データチェック処理部21₁、割り込み振分処理部22₁、割り込み処理部23₁、レジスタデータ読書き処理部24₁、割り込みベクタテーブル25₁、ページテーブル26₁、レジスタ退避領域27₁等から構成されている。

40

【0060】

図1に示したOS切替え処理部28₁は、データチェック処理部21₁、割り込み振分処理部22₁、割り込み処理部23₁、割り込みベクタテーブル25₁、ページテーブル26₁、レジスタ退避領域27₁等に対応するものである。AP30₁およびAP30₂は、OS20₁上で走行するアプリケーションプログラムである。

【0061】

一方、OS20₂は、OS20₁に併設されており、データチェック処理部21₂、割り込み振分処理部22₂、割り込み処理部23₂、レジスタデータ読書き処理部24₂、割り込みベクタテーブル25₂、ページテーブル26₂、レジスタ退避領域27₂等から構成されている。

50

【0062】

図1に示したOS切り替え処理部28₂ は、データチェック処理部21₂、割り込み振分処理部22₂、割り込み処理部23₂、割り込みベクタテーブル25₂、ページテーブル26₂、レジスタ退避領域27₂等に対応するものである。AP30₃およびAP30₄ は、OS20₂上で走行するアプリケーションプログラムである。

【0063】

ハードウェア10において、制御部11は、CPU等であり、プログラム実行により各部を制御する。物理メモリ12は、物理的に実在する大容量の記憶装置であり、図3に示したように、仮想記憶制御方式に用いられ、各種命令やデータ等を実際に記憶する。

【0064】

すなわち、本実施の形態1においては、物理メモリ12に対応して、仮想メモリ空間40₁および仮想メモリ空間40₂が仮想的に構築されている。仮想メモリ空間40₁は、OS20₁側に対応して設けられており、物理メモリ12のOS用物理メモリ領域12a₁およびAP用物理メモリ領域12b₁にマッピングされている。

【0065】

具体的には、OS用仮想メモリ空間40a₁は、OS20₁で利用されるメモリ空間であり、OS用物理メモリ領域12a₁にマッピングされている。AP用仮想メモリ空間40b₁は、AP30₁およびAP30₂で利用されるメモリ空間であり、AP用物理メモリ領域12b₁にマッピングされている。

【0066】

一方、仮想メモリ空間40₂は、OS20₂側に対応して設けられており、物理メモリ12のOS用物理メモリ領域12a₂およびAP用物理メモリ領域12b₂にマッピングされている。

【0067】

具体的には、OS用仮想メモリ空間40a₂は、OS20₂で利用されるメモリ空間であり、OS用物理メモリ領域12a₂にマッピングされている。AP用仮想メモリ空間40b₂は、AP30₃およびAP30₄で利用されるメモリ空間であり、AP用物理メモリ領域12b₂にマッピングされている。

【0068】

物理メモリ12では、物理的な記憶単位に物理アドレスが付与されている。一方、仮想メモリ空間40₁および仮想メモリ空間40₂では、プログラム中で用いられる論理アドレスによって命令やデータが特定される。仮想記憶制御方式では、ページング方式、セグメンテーション方式、ページング/セグメンテーション方式により、論理アドレスを物理アドレスに変換している。

【0069】

ページング方式では、アドレス変換がページと呼ばれるブロック単位(4キロバイト)で行われる。このため、OS20₁においては、仮想メモリ空間40₁の仮想ページが、物理メモリ12のどの物理ページに対応しているかを表すページテーブル(変換テーブル)26₁が設けられている。同様に、OS20₂においても、仮想メモリ空間40₂のページが、物理メモリ12のどのページに対応しているかを表すページテーブル(変換テーブル)26₂が設けられている。

【0070】

また、図4(b)に示したように、仮想メモリ空間40₁のZ番地(論理アドレス)には、OS20₁からOS20₂へ通信するデータをデバッグレジスタ15に書き込むデータ書込命令Aが記憶されている。さらに、仮想メモリ空間40₁のN番地には、OS20₁からOS20₂へ切り替えるための切替命令Aが記憶されている。

【0071】

一方、仮想メモリ空間40₂において、仮想メモリ空間40₁のN番地と同一のN番地には、OS20₂からOS20₁へ切り替えるための切替命令Bが記憶されている。また、仮想メモリ空間40₂のN+1番地には、デバッグレジスタ15に書き込まれ

10

20

30

40

50

たデータを読み出すデータ読出命令 B が記憶されている。

【0072】

図2に戻り、割り込みベクタテーブルレジスタ13は、割り込みに応じた割込番号を格納するレジスタである。この割込番号は、後述する割り込みベクタテーブル25₁ または割り込みベクタテーブル25₂ での割り込み処理ルーチンの論理アドレスに対応している。

【0073】

ページテーブルレジスタ14は、後述するページテーブル26₁ またはページテーブル26₂ へのページインデックスを格納するレジスタである。デバッグレジスタ15は、実行中のOS20₂ またはOS20₁ により使用されていない、OS間データ通信用レジスタ18として利用されるレジスタである。その他レジスタ16は、汎用レジスタ、フラグレジスタ等である。プログラムカウンタ17は、仮想メモリ空間から命令をフェッチする論理アドレスを1インクリメントする。

【0074】

OS20₁ において、データチェック処理部21₁ は、OS20₁ からOS20₂ へ通信するデータについて、不正なものであるかどうか等のチェックを実行する。このチェック結果が異常なものである場合には、アラームがあがり、一連の処理が中断される。

【0075】

割り込み振分処理部22₁ は、割り込み発生時に、割り込みベクタテーブルレジスタ13の割込番号に基づき、割り込みベクタテーブル25₁ を参照して、所定の割り込み処理ルーチンへジャンプさせる。なお、実際には、割り込み振分処理部22₁ の処理は、割り込み発生時に制御部11内部で実行される。

【0076】

割り込み処理部23₁ は、割り込み処理ルーチン、OS切り替え処理(OS20₁ からOS20₂)を実行する。レジスタデータ読書き処理部24₁ は、OS₁ がOS₂ に通信するデータをデバッグレジスタ15に書き込む処理(データを格納する処理)と、OS₂ からの通信データをデバッグレジスタ15から読み出す処理(データを取得する処理)とを実行する。

【0077】

割り込みベクタテーブル25₁ は、上述した割込番号毎の、割り込み処理に対応する論理アドレスを格納している。ページテーブル26₁ は、仮想メモリ空間40₁ (図3参照)の各仮想ページと、物理メモリ12の各物理ページとの対応関係を表すテーブルである。

【0078】

レジスタ退避領域27₁ は、OS切り替え時に、切り替え前のOSに対応するレジスタ(割り込みベクタテーブルレジスタ13、ページテーブルレジスタ14、その他レジスタ16)の内容を退避するための領域である。具体的には、OS20₁ からOS20₂ へ切り替えられる場合、レジスタ退避領域27₁ には、OS20₁ に対応するレジスタの内容が退避される。

【0079】

一方、OS20₂ において、データチェック処理部21₂ は、OS20₂ からOS20₁ へ通信するデータについて、不正なものであるかどうか等のチェックを実行する。このチェック結果が異常なものである場合には、アラームがあがり、一連の処理が中断される。

【0080】

割り込み振分処理部22₂ は、割り込み発生時に、割り込みベクタテーブルレジスタ13の割込番号に基づき、割り込みベクタテーブル25₂ を参照して、所定の割り込み処理ルーチンへジャンプさせる。なお、実際には、割り込み振分処理部22₂ の処理は、割り込み発生時に制御部11内部で実行される。

10

20

30

40

50

【0081】

割り込み処理部23₂は、割り込み処理ルーチン、OS切り替え処理(OS20₂からOS20₁)を実行する。レジスタデータ読書き処理部24₂は、OS₂がOS₁に通信するデータをデバッグレジスタ15に書き込む処理(データを格納する処理)と、OS₁からの通信データをデバッグレジスタ15から読み出す処理(データを取得する処理)とを実行する。

【0082】

割り込みベクタテーブル25₂は、上述した割込番号毎の、割り込み処理に対応する論理アドレスを格納している。ページテーブル26₂は、仮想メモリ空間40₂(図3参照)の各仮想ページと、物理メモリ12の各物理ページとの対応関係を表すテーブルである。

10

【0083】

レジスタ退避領域27₂は、OS切り替え時に、切り替え前のOSに対応するレジスタ(割り込みベクタテーブルレジスタ13、ページテーブルレジスタ14、その他レジスタ16)の内容を退避するための領域である。具体的には、OS20₂からOS20₁へ切り替えられる場合、レジスタ退避領域27₂には、OS20₂に対応するレジスタの内容が退避される。

【0084】

つぎに、図5を参照して、本実施の形態1の動作原理について説明する。同図の例では、OS20₁が動作状態にあり、OS20₂が待機状態にあるものとする。この状態で、OS20₁側で割り込みが発生すると、割り込みベクタテーブルレジスタ13の割込番号に基づいて、割り込みベクタテーブル25₁が参照され、仮想メモリ空間40₁のL番地より、割り込み処理ルーチンが実行される。

20

【0085】

以後、プログラムカウンタ17(図2参照)が1インクリメントされる毎に、仮想メモリ空間40₁の番地が1つ移行し、当該番地の命令が順次実行される。そして、仮想メモリ空間40₁のZ番地でデータ書込命令Aが実行され、OS20₂に通信するデータがデバッグレジスタ15に書き込まれる。その後、N番地で切替命令Aが実行され、OS20₁からOS20₂へ切り替えられる。

【0086】

そして、プログラムカウンタ17が1インクリメントされ、論理アドレスがN+1番地になると、仮想メモリ空間40₂のN+1番地のデータ読込命令Bが実行され、デバッグレジスタ15からデータが読み出される。なお、このデータ読込命令Bは、N+1番地以外のアドレスに記憶され、N+1番地の命令が実行された後に実行されることとしてもよい。

30

【0087】

以後、プログラムカウンタ17(図2参照)が1インクリメントされる毎に、仮想メモリ空間40₂の番地が1つ移行し、当該番地の命令が順次実行される。そして、仮想メモリ空間40₂のS番地でジャンプ命令が実行され、仮想メモリ空間40₂のN-M番地へジャンプされる。

40

【0088】

以後、プログラムカウンタ17(図2参照)が1インクリメントされる毎に、仮想メモリ空間40₂の番地が1つ移行し、当該番地の命令が順次実行される。そして、仮想メモリ空間40₂のP番地でデータ書込命令Bが実行され、OS20₁に通信するデータがデバッグレジスタ15に書き込まれる。その後、N番地で切替命令Bが実行され、OS20₂からOS20₁へ切り替えられる(切り戻される)。

【0089】

そして、プログラムカウンタ17が1インクリメントされ、論理アドレスがN+1番地になると、仮想メモリ空間40₁のN+1番地のデータ読込命令Aが実行され、デバッグレジスタ15からデータが読み出される。なお、このデータ読込命令Aは、N+1番地以

50

外のアドレスに記憶され、N + 1 番地の命令が実行された後に実行されることとしてもよい。

【0090】

その後、プログラムカウンタ17が1インクリメントされ、論理アドレスがN + 2 番地になると、IRETが実行され、割り込みから復帰される。なお、OS20₂ 側で割り込みが発生した場合も、上述と同様に動作する。

【0091】

つぎに、図6～図8を参照して、本実施の形態1の動作例について説明する。図6は、本実施の形態1の動作例を説明する図である。この動作例では、仮想メモリ空間40₁ および仮想メモリ空間40₂ の各論理アドレスには、同図に示した処理に対応する各種命令が割り当てられている。

10

【0092】

同図の例では、OS20₁ が動作状態にあり、OS20₂ が待機状態にあるものとする。この状態で、OS20₁ 側で割り込みが発生すると、割り込み振分処理部22₁ は、▲1▼で、割り込みベクタテーブルレジスタ13の割込番号に基づいて、割り込みベクタテーブル25₁ を参照し、当該割り込み処理へジャンプする。

【0093】

これにより、割り込み処理部23₁ は、▲2▼で、仮想メモリ空間40₁ のL番地より割り込み処理ルーチンを実行する。以後、プログラムカウンタ17（図2参照）が1インクリメントされる毎に、仮想メモリ空間40₁ の番地が1つ移行し、当該番地の命令が順次実行される。

20

【0094】

そして、仮想メモリ空間40₁ のY番地においては、仮想メモリ空間40₁ におけるOS切り替え処理の前に割り込み禁止命令が実行される。割り込み禁止命令が実行されると、他の割り込みを受け付けない状態となる。この割り込み禁止命令は、OS切り替え処理を実行中に、より優先度が高い割り込みが多重的に入ることを防止するために実行されるものである。

【0095】

そして、OS切り替え処理（レジスタをレジスタ退避領域に退避）では、Y + 1 番地で、OS20₁ に対応する割り込みベクタテーブルレジスタ13、ページテーブルレジスタ14およびその他レジスタ16の内容がレジスタ退避領域27₁ に退避される。

30

【0096】

続いてのZ - 1 番地におけるOS切替え処理（OS間通信データチェック）では、OS20₁ からOS20₂ へ通信するデータの不正チェック等をおこなう。チェック結果が異常である場合には、アラームがあがり、一連の処理が中断される。

【0097】

この場合、チェック結果が正常であるものとし、Z番地のOS切替え処理（OS間通信データチェック）では、デバッグレジスタ15にOS20₁ からOS20₂ へ通信するデータを書き込む。

【0098】

そして、OS切り替え処理（IDTR切り替え命令）では、割り込みベクタテーブルレジスタ13が、OS20₁ 用からOS20₂ 用に切り替えられる。つぎのOS切り替え処理（ページテーブルレジスタ変更命令）では、仮想メモリ空間40₁ のN番地で、ページテーブルレジスタ14がOS20₁ 用からOS20₂ 用に変更される。これにより、OS20₁ からOS20₂ へ切り替えられる（▲3▼）。

40

【0099】

続いてのOS切り替え処理（レジスタからOS間通信データを読み込む）では、仮想メモリ空間40₂ のN + 1 番地で、デバッグレジスタ15からデータを読み込む。

【0100】

その後のOS切り替え処理（レジスタ退避領域からレジスタを復帰）では、N + 2 番地に

50

において、以前にレジスタ退避領域 27_2 に退避されていた $OS20_2$ 用のレジスタの内容が割り込みベクタテーブルレジスタ 13 、ページテーブルレジスタ 14 およびその他レジスタ 16 にそれぞれ復帰される。そして、 $N+3$ 番地において、割り込み許可命令が実行される。割り込み許可命令が実行されると、他の割り込みを受け付ける状態となる（▲4▼）。

【0101】

そして、割り込み処理部 23_2 は、割り込み処理ルーチンを順次実行する。そして、仮想メモリ空間 40_2 の S 番地でジャンプ命令が実行され、仮想メモリ空間 40_2 の $N-M$ 番地へジャンプされる（▲5▼）。

【0102】

その後、仮想メモリ空間 40_2 の $N-M$ 番地における割り込み禁止命令が実行され、他の割り込みを受け付けられない状態となる。そして、 $N-M+1$ 番地の OS 切り替え処理（レジスタをレジスタ退避領域に退避）では、 $OS20_2$ に対応する割り込みベクタテーブルレジスタ 13 、ページテーブルレジスタ 14 およびその他レジスタ 16 の内容がレジスタ退避領域 27_2 に退避される。

【0103】

続いての $P-1$ 番地の OS 切り替え処理（ OS 間通信データチェック）では、 $OS20_2$ から $OS20_1$ へ通信するデータの不正チェック等をおこなう。チェック結果が異常である場合には、アラームがあがり、一連の処理が中断される。

【0104】

この場合、チェック結果が正常であるものとし、 P 番地の OS 切り替え処理（レジスタに OS 間通信データを書き込む）では、デバッグレジスタ 15 に $OS20_2$ から $OS20_1$ へ通信するデータを書き込む。そして、 OS 切り替え処理（ $IDTR$ 切り替え命令）では、割り込みベクタテーブルレジスタ 13 が、 $OS20_2$ 用から $OS20_1$ 用に切り替えられる（▲6▼）。

【0105】

続いての OS 切り替え処理（ページテーブルレジスタ変更命令）では、仮想メモリ空間 40_2 の N 番地で、ページテーブルレジスタ 14 が $OS20_2$ 用から $OS20_1$ 用に変更される。これにより、 $OS20_2$ から $OS20_1$ へ切り替えられる（▲7▼）。

【0106】

その後の OS 切り替え処理（レジスタから OS 間通信データを読み込む）では、仮想メモリ空間 40_1 の $N+1$ 番地において、デバッグレジスタ 15 からデータを読み込む。

【0107】

そして、 OS 切り替え処理（レジスタ退避領域からレジスタを復帰）では、仮想メモリ空間 40_1 の $N+2$ 番地において、先にレジスタ退避領域 27_1 に退避されていた $OS20_1$ 用のレジスタの内容が割り込みベクタテーブルレジスタ 13 、ページテーブルレジスタ 14 およびその他レジスタ 16 にそれぞれ復帰される。そして、 $N+3$ 番地において、割り込み許可命令が実行される。割り込み許可命令が実行されると、他の割り込みを受け付ける状態となる。

【0108】

つぎに、割り込み処理部 23_1 は、割り込み処理ルーチンを順次実行する。そして、仮想メモリ空間 40_1 の X 番地で $IRET$ （割り込み復帰命令）が実行され、処理ルーチンが割り込み処理ルーチンから通常処理ルーチンへ復帰される（▲8▼）。

【0109】

図7および図8は、上記動作例を説明するフローチャートである。同図において、割り込みが発生すると、ステップ $SA1$ では、 $OS20_1$ のアプリケーション走行が中止され、割り込み振分処理部 22_1 が起動される。ステップ $SA2$ では、 $OS20_1$ の割り込み振分処理部 22_1 が割り込みに対応する割込番号を割り込みベクタテーブルレジスタ 13 から取得する。

【0110】

10

20

30

40

50

ステップ S A 3 では、割り込み振分処理部 2 2₁ により、割り込みベクタテーブル 2 5₁ が参照され、仮想メモリ空間 4 0₁ における割り込み処理ルーチンのある論理アドレスにジャンプされる（図 6 の▲ 1 ▼）。ステップ S A 4 では、割り込み処理ルーチンが実行される（図 6 の▲ 2 ▼）。

【 0 1 1 1 】

ステップ S A 5 では、割り込み禁止命令が実行される（図 6 の Y 番地）。ステップ S A 6 では、O S 切り替え処理（レジスタをレジスタ退避領域に退避）が実行される。ステップ S A 7 では、O S 切り替え処理（O S 間通信データチェック）が実行され、O S 2 0₂ へ通信するデータのチェックがおこなわれる（図 6 の Z - 1 番地）。なお、チェック結果が異常である場合には、アラームがあがり、一連の処理が中断される。

10

【 0 1 1 2 】

この場合、チェック結果が正常であるものとし、ステップ S A 8 では、O S 切り替え処理（レジスタに O S 間通信データを書き込む）が実行され、デバッグレジスタ 1 5 に O S 2 0₂ へ通信するデータを書き込む（図 6 の Z 番地）。

【 0 1 1 3 】

ステップ S A 9 では、O S 切り替え処理（I D T R 切り替え命令）が実行される。ステップ S A 1 0 では、O S 切り替え処理（ページテーブルレジスタ変更命令）が実行され（図 6 の▲ 3 ▼）、O S 2 0₁ から O S 2 0₂ へ切り替わる。

【 0 1 1 4 】

ステップ S A 1 1 では、O S 2 0₂ で O S 切り替え処理（レジスタから O S 間通信データを読み込む）が実行される（図 6 の N + 1 番地）。ステップ S A 1 2 では、O S 切り替え処理（レジスタ退避領域からレジスタを復帰）が実行される（図 6 の N + 2 番地）。

20

【 0 1 1 5 】

ステップ S A 1 3 では、割り込み許可命令が実行される（図 6 の N + 3 番地）。ステップ S A 1 4 では、割り込み処理ルーチンが実行される。ステップ S A 1 5 では、ジャンプ命令が実行され、N - M 番地にジャンプされる（図 6 の▲ 5 ▼）。

【 0 1 1 6 】

図 8 に示したステップ S A 1 6 では、割り込み禁止命令が実行される（図 6 の N - M 番地）。ステップ S A 1 7 では、O S 切り替え処理（レジスタをレジスタ退避領域に退避）が実行される。ステップ S A 1 8 では、O S 切り替え処理（O S 間通信データチェック）が実行され、O S 2 0₁ へ通信するデータのチェックがおこなわれる（図 6 の P - 1 番地）。なお、チェック結果が異常である場合には、アラームがあがり、一連の処理が中断される。

30

【 0 1 1 7 】

この場合、チェック結果が正常であるものとし、ステップ S A 1 9 では、O S 切り替え処理（レジスタに O S 間通信データを書き込む）が実行され、デバッグレジスタ 1 5 に O S 2 0₂ へ通信するデータを書き込む（図 6 の P 番地）。

【 0 1 1 8 】

ステップ S A 2 0 では、O S 切り替え処理（I D T R 切り替え命令）が実行される。ステップ S A 2 1 では、O S 切り替え処理（ページテーブルレジスタ変更命令）が実行され（図 6 の▲ 7 ▼）、O S 2 0₂ から O S 2 0₁ へ切り替わる。

40

【 0 1 1 9 】

ステップ S A 2 2 では、O S 2 0₁ で O S 切り替え処理（レジスタから O S 間通信データを読み込む）が実行される（図 6 の N + 1 番地）。ステップ S A 2 3 では、O S 切り替え処理（レジスタ退避領域からレジスタを復帰）が実行される（図 6 の N + 2 番地）。

【 0 1 2 0 】

ステップ S A 2 4 では、割り込み許可命令が実行される（図 6 の N + 3 番地）。ステップ S A 2 5 では、割り込み処理ルーチンが実行される。ステップ S A 2 6 では、I R E T（割り込み復帰命令）が実行され、割り込みから復帰される。

【 0 1 2 1 】

50

以上説明したように、本実施の形態１によれば、OS 20₁ からOS 20₂ へ（または、OS 20₂ からOS 20₁ へ）通信するデータをデバッグレジスタ15に格納し、OS 20₁ からOS 20₂ へ（または、OS 20₂ からOS 20₁ へ）切り替えが実行された場合に、OS 20₂ （または、OS 20₁ ）がデバッグレジスタ15からデータを読み込むこととしたので、デバッグレジスタ15に格納されるデータサイズが制限されているため、不正なデータやウィルスプログラムがOS 20₁ とOS 20₂ との間で伝播しにくく、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができる。

【0122】

また、本実施の形態１によれば、通信対象のデータの正常性をデータチェック処理部21₁ およびデータチェック処理部21₂ でチェックし、正常である場合にのみ通信処理を継続させることとしたので、マルチオペレーティングシステムのセキュリティ、信頼性をさらに向上させることができる。

【0123】

また、本実施の形態１によれば、OSにより使用されていないレジスタを利用するだけであるので、何ら特別な装置や回路を必要とせず、市販のパーソナルコンピュータでも用意に実現することができる。

【0124】

（実施の形態２）

さて、前述した実施の形態１では、OS 20₁ とOS 20₂ との間でレジスタを介してデータを通信する場合を示したが、データを通信する際に、データサイズがレジスタに格納できるサイズである場合には、レジスタを利用したデータ通信をおこない、レジスタに格納できないサイズである場合には、別の方法でそのデータを通信するよう構成してもよい。

【0125】

以下では、レジスタに格納できないデータサイズである場合に、レジスタによる通信からNIC（Network Interface Card）を利用する通信に切り替えて通信をおこなう構成例について説明する。

【0126】

図9は、本実施の形態２の構成を示すブロック図である。この図に示したマルチオペレーティングシステムは、NIC（Network Interface Card）60、NICデバイスドライバ70₁、NICデバイスドライバ70₂、OS 20₁、OS 20₂、AP 30₁～30₄、ネットワーク50および図2に示したハードウェア10を有している（図示は省略）。

【0127】

ここで、OS 20₁ およびOS 20₂ は、図2に示したOS 20₁ およびOS 20₂ と同様のものであり、さらにデータサイズ判定部29₁ およびデータサイズ判定部29₂ をそれぞれ有している。

【0128】

また、OS切り替え処理部28₁ は、図2に示したデータチェック処理部21₁、割り込み振分処理部22₁、割り込み処理部23₁、割り込みベクタテーブル25₁、ページテーブル26₁、レジスタ退避領域27₁等に対応するものである。OS切り替え処理部28₂ は、図2に示したデータチェック処理部21₂、割り込み振分処理部22₂、割り込み処理部23₂、割り込みベクタテーブル25₂、ページテーブル26₂、レジスタ退避領域27₂等に対応するものである。

【0129】

同マルチオペレーティングシステムでは、OS 20₁ からOS 20₂ へ、またはOS 20₂ からOS 20₁ への切り替えが割り込み処理ルーチンの中で実行される。割り込みの発生要因としては、OS間のデータの通信要求、タイマ（図示略）による定期的な切り替え要求等が挙げられる。

10

20

30

40

50

【0130】

このマルチオペレーティングシステムでは、従来のように共通の制御プログラムや、共用メモリ等を介さずに、OS間データ通信用レジスタ18あるいはNIC60を用いて、高いセキュリティを保持した状態でOS20₁ とOS20₂ との間でデータの受け渡しを実現する点に特徴がある。

【0131】

以下、各構成要素について詳述する。NIC60は、例えば、LAN (Local Area Network) カードであり、通信インタフェース機能を備えている。このNIC60は、後述するNICデバイスドライバ70₁ およびNICデバイスドライバ70₂ により制御される。

10

【0132】

NIC60において、NIC送信処理部61は、パケットを送信する機能を備えている。送信バッファ62は、NIC送信処理部61から送信されるパケットを一時的に格納する。NIC受信処理部63は、ネットワーク50よりパケットを受信する機能を備えている。受信バッファ64は、NIC受信処理部63により受信されたパケットを一時的に格納する。

【0133】

送信バッファレジスタ65は、後述する送信バッファ72₁ または送信バッファ72₂ のいずれかに対応する値（アドレス）を格納するレジスタである。受信バッファレジスタ66は、後述する受信バッファ74₁ または受信バッファ74₂ のいずれかに対応する値（アドレス）を格納するレジスタである。

20

【0134】

NICデバイスドライバ70₁ は、OS20₁ の一部の機能を実現するものであり、通信時にNIC60を制御する機能、送信バッファレジスタ65や受信バッファレジスタ66の値を書き換える機能等を備えている。

【0135】

NICデバイスドライバ70₁ において、送信処理部71₁ は、OS20₁ からのデータを送信する機能を備えている。送信バッファ72₁ は、OS20₁ からのデータを一時的に格納する。受信処理部73₁ は、OS20₁ 宛のデータを受信する機能を備えている。受信バッファ74₁ は、OS20₁ 宛のデータを一時的に格納する。

30

【0136】

一方、NICデバイスドライバ70₂ は、OS20₂ の一部の機能を実現するものであり、通信時にNIC60を制御する機能、送信バッファレジスタ65や受信バッファレジスタ66の値を書き換える機能等を備えている。

【0137】

ここで、OS20₁ には、IPアドレスとして、例えば、192.168.1.3が付与されている。一方、OS20₂ には、別のIPアドレスとして、例えば、192.168.1.4が付与されている。

【0138】

つぎに、NIC60を利用してデータの通信をおこなう場合の動作原理について、図10に示したブロック図を参照して説明する。ここでは、NIC60を介して、OS20₁ からOS20₂ へ通信する場合について説明する。

40

【0139】

同図においては、OS20₁ が実行中であって、送信バッファレジスタ66に送信バッファ72₁ に対応する値が格納されており、かつ受信バッファレジスタ65に受信バッファ74₁ に対応する値が格納されている状態にあるものとする。

【0140】

この状態で、(1)では、NICデバイスドライバ70₁ の送信処理部71₁ は、OS20₁ からのデータを送信バッファ72₁ に格納する。このデータは、OS20₁ からOS20₂ へ送信される。従って、当該データの送信先IPアドレスは、OS2

50

0₂ に付与された192.168.1.4である。

【0141】

(2)では、送信処理部71₁ は、NIC60の受信バッファレジスタ65の値を受信バッファ74₁ から受信バッファ74₂ に書き換える。(3)では、NIC送信処理部61は、送信バッファレジスタ66を参照して、送信バッファ72₁ にアクセスした後、送信バッファ72₁ から送信バッファ62ヘデータをコピーする。

【0142】

(4)では、NIC送信処理部61は、送信バッファ62からデータを読み出し、これをネットワーク50へ送信する。そして、当該データは、NIC受信処理部63に受信された後、受信バッファ64に格納される。

10

【0143】

(5)では、NIC受信処理部63は、受信バッファレジスタ65を参照して、受信バッファ74₂ にアクセスした後、受信バッファ64から受信バッファ74₂ ヘデータをコピーする。

【0144】

(6)では、OS切替え処理部28₁ は、OSをOS20₁ からOS20₂ へ切り替える。(7)では、受信処理部73₂ は、受信バッファ74₂ からデータを読み出し、このデータを切り替え後のOS20₂ へ渡す。

【0145】

このように、NIC60を介しての通信の動作では、従来のようにOS間で共通の制御プログラムや共有メモリ等を介さずに、高いセキュリティを保持した状態で、OS間通信を実現することができる。

20

【0146】

つぎに、本実施の形態2のOS間データ通信の動作例を説明する。図11および図12は、本実施の形態2のOS間データ通信の動作例を示すフローチャートである。この動作例では、OS間データ通信用レジスタ18またはNIC60による通信をデータのサイズにより切り替えておこなう。なお、以下では実施の形態1と同様、デバッグレジスタ15をOS間データ通信用レジスタ18として利用する場合について説明する。

【0147】

図11において、割り込みが発生すると、ステップSB1では、OS20₁ のアプリケーション走行が中止され、割り込み振分処理部22₁ が起動される。ステップSB2では、OS20₁ の割り込み振分処理部22₁ が割り込みに対応する割込番号を割り込みベクタテーブルレジスタ13から取得する。

30

【0148】

ステップSB3では、割り込み振分処理部22₁ により、割り込みベクタテーブル25₁ が参照され、仮想メモリ空間40₁ における割り込み処理ルーチンのある論理アドレスにジャンプされる。ステップSB4では、割り込み処理ルーチンが実行される。

【0149】

ステップSB5では、割り込み禁止命令が実行される。ステップSB6では、OS切り替え処理(レジスタをレジスタ退避領域に退避)が実行される。ステップSB7では、OS切り替え処理(OS間通信データチェック)が実行され、OS20₂ へ通信するデータのチェックがおこなわれる。なお、チェック結果が異常である場合には、アラームが上がり、一連の処理が中断される。

40

【0150】

この場合、チェック結果が正常であるものとし、ステップSB8では、OS切り替え処理(OS間通信データのデータサイズチェック)が実行され、デバッグレジスタ15にOS2₂ へ通信するデータを書き込みできるかどうかを調べる。

【0151】

ステップSB9の判定結果が「Yes」で、書き込み可能である場合には、ステップSB10で、OS切り替え処理(レジスタにOS間通信データを書き込む)が実行され、デバ

50

ッグレジスタ15にOS20₂へ通信するデータを書き込む。ステップSB12では、OS切り替え処理(IDTR切り替え命令)が実行される。

【0152】

ステップSB9の判定結果が「No」で、書き込み不可能である場合には、ステップSB11で、OS切り替え処理(NIC60を用いた通信データ送信処理)が実行される。この処理では、図10に示した(1)から(5)までの処理がおこなわれ、その後、ステップSB12に移行する。

【0153】

ステップSB13では、OS切り替え処理(ページテーブルレジスタ変更命令)が実行され、OS20₁からOS20₂へ切り替わる。ステップSB14では、デバッグレジスタ15を用いた通信であるかどうかを判定する。

10

【0154】

例えば、NIC60を用いて通信する場合には、通信データとともに判定フラグを送信し、その判定フラグをOS20₂が受信してNIC60による通信を検出する。判定フラグが受信されない場合には、デバッグレジスタ15を用いた通信であるとの判定をおこなう。なお、これに限らず他の判定方法を用いてもよい。

【0155】

ステップSB14の判定結果が「Yes」である場合には、ステップSB15では、OS20₂でOS切り替え処理(レジスタからOS間通信データを読み込む)が実行される。ステップSB17では、OS切り替え処理(レジスタ退避領域からレジスタを復帰)が

20

【0156】

ステップSB14の判定結果が「No」である場合には、ステップSB16で、OS切り替え処理(NIC60を用いた通信データ受信処理)が実行される。この処理では、図10に示した(7)の処理がおこなわれ、その後、ステップSB17に移行する。

【0157】

ステップSB18では、割り込み許可命令が実行される。ステップSB19では、割り込み処理ルーチンが実行される。ステップSB20では、ジャンプ命令が実行され、N-M番地にジャンプされる。

【0158】

30

図12に示したステップSB21では、割り込み禁止命令が実行される。ステップSB22では、OS切り替え処理(レジスタをレジスタ退避領域に退避)が実行される。ステップSB23では、OS切り替え処理(OS間通信データチェック)が実行され、OS20₁へ通信するデータのチェックをおこなう。なお、チェック結果が異常である場合には、アラームがあがり、一連の処理が中断される。

【0159】

この場合、チェック結果が正常であるものとし、ステップSB24では、OS切り替え処理(OS間通信データのデータサイズチェック)が実行され、デバッグレジスタ15にOS₁へ通信するデータを書き込みできるかどうかを調べる。

【0160】

40

ステップSB25の判定結果が「Yes」で、書き込み可能である場合には、ステップSB26で、OS切り替え処理(レジスタにOS間通信データを書き込む)が実行され、デバッグレジスタ15にOS20₁へ通信するデータを書き込む。ステップSB28では、OS切り替え処理(IDTR切り替え命令)が実行される。

【0161】

ステップSB25の判定結果が「No」で、書き込み不可能である場合には、ステップSB27で、OS切り替え処理(NIC60を用いた通信データ送信処理)が実行される。この処理では、図10に示した(1)から(5)までの処理と同様の方法で、OS20₂からOS20₁への通信データの送信処理がおこなわれ、その後、ステップSB28に移行する。

50

【0162】

ステップS B 2 9では、OS切り替え処理（ページテーブルレジスタ変更命令）が実行され、OS 2 0₂ からOS 2 0₁ へ切り替わる。ステップS B 3 0では、デバッグレジスタ15を用いた通信であるかどうかを判定する。

【0163】

例えば、NIC 6 0を用いて通信する場合には、通信データとともに判定フラグを送信し、その判定フラグをOS 2 0₁ が受信してNIC 6 0による通信を検出する。判定フラグが受信されない場合には、デバッグレジスタ15を用いた通信であるとの判定をおこなう。なお、これに限らず他の判定方法を用いてもよい。

【0164】

ステップS B 3 0の判定結果が「Yes」である場合には、ステップS B 3 1では、OS 2 0₁ でOS切り替え処理（レジスタからOS間通信データを読み込む）が実行される。ステップS B 3 3では、OS切り替え処理（レジスタ退避領域からレジスタを復帰）が実行される。

【0165】

ステップS B 3 0の判定結果が「No」である場合には、ステップS B 3 2で、OS切り替え処理（NIC 6 0を用いた通信データ受信処理）が実行される。この処理では、図1 0に示した（7）の処理と同様の方法で、OS 2 0₁ が通信データの受信処理をおこない、その後、ステップS B 3 3に移行する。

【0166】

ステップS B 3 4では、割り込み許可命令が実行される。ステップS B 3 5では、割り込み処理ルーチンが実行される。ステップS B 3 6では、IRET（割り込み復帰命令）が実行され、割り込みから復帰される。

【0167】

以上説明したように、本実施の形態2によれば、データを通信する際に、データサイズがデバッグレジスタ15に格納できるサイズである場合には、デバッグレジスタ15を利用したデータ通信をおこない、デバッグレジスタ15に格納できないサイズである場合には、NIC 6 0を用いてそのデータを通信することとしたので、従来のように共通の制御プログラムや、共用メモリ等を介さずに、OS間データ通信用レジスタ18あるいはNIC 6 0を用いて、高いセキュリティを保持した状態でOS 2 0₁ とOS 2 0₂ との間でデータの受け渡しをおこなうことができる。

【0168】

また、本実施の形態2によれば、通信対象のデータの正常性をチェックし、正常である場合にのみ通信処理を継続させることとしたので、マルチオペレーティングシステムのセキュリティ、信頼性をさらに向上させることができる。

【0169】

ここで、本実施の形態2では、データサイズが大きく、デバッグレジスタ15に格納できない場合に、NIC 6 0を用いて通信をおこなうこととしたが、それに限定されず、従来のように共通の制御プログラムや、共用メモリ等を介してデータ通信をおこなうこととしてもよい。

【0170】

上記において、共通の制御プログラムや共用メモリ等を介してデータ通信をおこなう場合には、セキュリティが低下してしまうものの、データサイズが小さく、デバッグレジスタ15を用いて通信する場合には、依然高いセキュリティを保持した状態でOS 2 0₁ とOS 2 0₂ との間でデータの受け渡しをおこなうことができる。

【0171】

図13（a）～図13（d）は、前述した実施の形態1または2の応用例1～4を説明する図である。図13（a）に示した応用例1は、新旧OSを共存させ、システム更改時に利用する例である。新OSは、例えば、OS 2 0₁ に対応している。一方、旧OSは、OS 2 0₁ に対応している。

10

20

30

40

50

【0172】

図13(b)に示した応用例2は、ソース公開OSを活用し、ソース非公開OSのリリースを待たずに、ソース公開OS側で新機能をスピード開発する例である。ソース非公開OSは、ソースコードが公開されていないオペレーティングシステムであり、例えば、OS20₁に対応している。一方、ソース公開OSは、ソースコードが公開されているオペレーティングシステムであり、OS20₂に対応している。

【0173】

図13(c)に示した応用例3は、専用OSと汎用OSとを共存させる例である。専用OSは、リアルタイム性等に特化する機能を分担し、例えば、OS20₁に対応している。一方、汎用OSは、マイクロソフト社のWindows(登録商標)等であり、GUI機能を分担し、OS20₂に対応している。

10

【0174】

図13(d)に示した応用例4は、資源を分割する例であり、OS1とOS2の使用目的により使用方法が異なる例である。OS1は、例えば、OS20₁に対応している。一方、OS2は、OS20₂に対応している。

【0175】

図14は、実施の形態1または2をシステム移行に適用した場合を説明する図である。同図において、従来の移行作業では、一度に、旧端末に実装されている旧OSの全モジュールを新端末の新OSに移行させる必要があり、安全面で不安が残る。

【0176】

これに対して、マルチオペレーティングシステムがあると、旧端末に実装されている旧OSの各モジュールを中間端末の旧OSに安全を確認しながら移行させる。つぎに、中間端末において、旧OSの各モジュールを新OSに安全を確認しながら移行させる。

20

【0177】

つぎに、中間端末の新OSの全モジュールを、新端末の新OSに一度に移行させる。この場合、新OS間での移行であるため、問題が発生しない。マルチOSによる移行は、ある特定のモジュールに急いで新機能をつける場合に有効である。

【0178】

図15は、実施の形態1または2を高セキュリティゲートウェイに適用した場合を説明する図である。同図において、ハードウェアは、マルチオペレーティングシステム(OS1およびOS2)を備えており、NIC(ネットワークインタフェースカード)を経由してインターネットに接続されている。このハードウェアは、高セキュリティゲートウェイとして機能する。

30

【0179】

OS1は、ユーザが使用するAP(アプリケーションプログラム)1を管理するとともに、通信ログをDK(ディスク)1に蓄積する。一方、OS2は、インターネットからの通信パケットを監視し、監視ログをDK2に蓄積する。

【0180】

また、OS2では、NICを直接制御し、通信を行う。このため、OS2は、OS1の通信を支援するため、NICの対ソフトウェア提供インタフェースを疑似した疑似NIC-I/FをOS1に提供している。AP2は、パケット監視ログ収集用のアプリケーションプログラムであり、OS2上で動作する。

40

【0181】

また、AP2は、通信パケットを外から見るだけで、通信パケットに含まれる実行コードを処理しないため、ウイルスに感染しない。DK2に蓄積される監視ログは、悪意の第三者による改竄がなされないようになっている。従って、攻撃の痕跡を残すことが可能となる。

【0182】

ここで、ユーザの環境(OS1等)に対して、セキュリティの攻撃が行われた場合、OS1の通信ログが改竄されることが考えられる。しかしながら、実施の形態1または2では

50

、マルチオペレーティングシステムにより、OS 1とOS 2の監視ログが別々に管理されるため、攻撃者の追跡を行うことが可能となる。これにより、当該セキュリティゲートウェイへの攻撃を抑止する効果が期待できる。

【0183】

図16は、実施の形態1または2をデスクトップGrid端末に適用した場合を説明する図である。同図において、ハードウェアは、マルチオペレーティングシステム（OS 1およびOS 2）を備えており、NICを経由してインターネットに接続されている。インターネットには、Gridサーバが接続されている。ハードウェアは、デスクトップGrid端末として機能する。

【0184】

デスクトップGrid端末は、ユーザが計算機を利用しない間に、大きな計算の一部を割り当てて計算を実現しようとするデスクトップGrid計算を行うための端末である。ここで、ユーザ側から見ると、内容が不明な上記計算が自身の計算機環境に及ぼす悪影響が心配となる。

【0185】

そこで、同図では、自身の計算機環境をOS 1で管理し、Grid計算の処理環境をOS 2で管理することにより、上記悪影響を排除できる。つまり、Grid計算で利用されるデータやプログラムは、全てOS 2の制御下のみで管理され実行される。一方、OS 1の制御下にあるDK 1やMEM（メモリ）1という計算機資源には、アクセスが許可されない。従って、Grid計算のプログラムからの悪影響が排除される。

【0186】

図17は、実施の形態1または2を遠隔管理端末に適用した場合を説明する図である。同図において、ハードウェアは、マルチオペレーティングシステム（OS 1およびOS 2）を備えており、NICを経由してネットワークに接続されている。ネットワークには、システム管理者マシンや他のマシンが接続されている。ハードウェアは、遠隔管理端末として機能する。

【0187】

同図において、ユーザが管理できる範疇をOS 1に制限し、OS 2の管理をネットワークを介してシステム管理者マシンで行うように構成されている。これにより、オフィス環境などで利用するパーソナルコンピュータのデフォルト環境を、システム管理者がOS 2の管理下で構築し、一方、ユーザ個人の好みや状況に応じて利用する環境を、ユーザがOS 1の管理下で構築することができる。

【0188】

したがって、ユーザ個人の環境設定により、システム側で用意した環境が動作不具合になることが防止される。OS 2は、システム管理者マシンでシステム管理者により管理され、システム側で設計された環境を提供する。ユーザは、該環境を利用する場合、OS 2のファイル情報をOS 1に読み込んで起動するか、または、OS 2に起動を依頼してクライアント／サーバの形態で実行する。

【0189】

図18は、実施の形態1または2を高効率ネットサービス提供端末に適用した場合を説明する図である。同図において、ハードウェアは、マルチオペレーティングシステム（OS 1およびOS 2）を備えており、NICを経由してネットワークに接続されている。ネットワークには、コンテンツプロバイダサーバや他のマシンが接続されている。ハードウェアは、高効率ネットサービス提供端末として機能する。

【0190】

同図においては、高効率ネットサービス提供端末は、遠隔管理端末（図17参照）と同様にして、一方のOS 1をユーザの管理下、他方のOS 2をネットサービスの管理下として、例えば、封切り前のコンテンツを事前にOS 2の管理下（DK 2）に配信しておき、封切り時刻にOS 1の管理下のDK 1からのコンテンツの即時利用を実現する端末である。

【0191】

10

20

30

40

50

コンテンツは、ネットワークを介して、コンテンツプロバイダサーバからOS 2の管理下のDK 2に配信された後、ユーザの希望により、DK 2からOS 1の管理下のDK 1へ当該コンテンツが提供され、即時利用が可能となる。このように、コンテンツプロバイダサーバでは、事前配信により、ダウンロードアクセスの集中が防止される。

【0192】

図19は、実施の形態1または2を高セキュリティWebサービス提供サーバに適用した場合を説明する図である。同図において、ハードウェアは、マルチオペレーティングシステム(OS 1およびOS 2)を備えており、NICを経由してネットワークに接続されている。ネットワークには、Web閲覧端末が接続されている。ハードウェアは、高セキュリティWebサービス提供サーバとして機能する。

10

【0193】

同図の高セキュリティWebサービス提供サーバにおいては、外部からアクセスできる環境がOS 2で、ローカルユーザだけがアクセスできる環境がOS 1で構築される。

【0194】

例えば、Web公開コンテンツや利用ログは、OS 2の管理下のDK 2に格納される。一方、公開したくないデータ等は、OS 1の管理下のDK 1に格納される。この場合、設定ミス等により、公開したくない情報を誤ってWeb上で公開してしまうという事態が回避される。また、外部から悪意の第三者による攻撃をOS 2側が受けた場合であっても、OS 1では、ネットワーク機能を除き、動作することが可能となる。

【0195】

20

以上本発明にかかる実施の形態1および2について図面を参照して詳述してきたが、具体的な構成例はこれらの実施の形態1および2に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。

【0196】

例えば、前述した実施の形態1および2においては、前述したマルチオペレーティングシステム制御、制御等を実現するためのプログラムを図20に示したコンピュータ読み取り可能な記録媒体200に記録して、この記録媒体200に記録されたプログラムを同図に示したコンピュータ100に読み込ませ、実行することにより各機能を実現してもよい。

【0197】

同図に示したコンピュータ100は、上記プログラムを実行するCPU 110と、キーボード、マウス等の入力装置120と、各種データを記憶するROM (Read Only Memory) 130と、演算パラメータ等を記憶するRAM (Random Access Memory) 140と、記録媒体200からプログラムを読み取る読取装置150と、ディスプレイ、プリンタ等の出力装置160と、装置各部を接続するバス170とから構成されている。

30

【0198】

CPU 110は、読取装置150を経由して記録媒体200に記録されているプログラムを読み込んだ後、プログラムを実行することにより、前述した機能を実現する。なお、記録媒体200としては、光ディスク、フレキシブルディスク、ハードディスク等が挙げられる。

40

【0199】

また、実施の形態1および2においては、2つのオペレーティングシステム間の切り替え方法として、仮想メモリ空間の論理アドレスを適切に設定し、割り込みベクタテーブルレジスタとページテーブルレジスタを変更することによりオペレーティングシステムを切り替える方法について説明したが、本発明はこれに限られるものではなく、従来の仮想計算機方式あるいはマイクロカーネル方式によりオペレーティングシステムを切り替えてもよい。

【0200】

また、実施の形態1および2においては、マルチオペレーティングシステムとして、図1に示した二つのOS 20₁、OS 20₂を有する構成例について説明したが、三つ以

50

上のOSを有する構成例も本発明に含まれる。

【0201】

例えば、OS1、OS2、OS3、・・・、OSnというn個のOSを有する構成の場合には、OS1走行中に割り込み(1)が発生した場合にOS1からOS2に切り替え、OS1走行中に割り込み(2)が発生した場合にOS1からOS3に切り替え、以下同様にして、OS1走行中に割り込み(n-1)が発生した場合にOS1からOSnに切り替えるように制御すればよい。

【0202】

【発明の効果】

以上説明したように、本発明によれば、第1のオペレーティングシステムの実行中に所定のレジスタに通信対象となるデータを格納し、第1のオペレーティングシステムから第2のオペレーティングシステムに切り替えがなされた場合に、所定のレジスタから通信対象となるデータを取得することとしたので、共有メモリを介さずに、格納できるデータのサイズが制限されたレジスタをオペレーティングシステム間の通信に用いることで、不正なデータの通信による各オペレーティングシステムの異常動作の可能性を回避することができ、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができるという効果を奏する。

【0203】

また、本発明によれば、所定のレジスタに通信対象となるデータが格納された際に、第1のオペレーティングシステムに対応する第1の仮想メモリ空間の論理アドレスNにあらかじめ仮想記憶された、第1のオペレーティングシステムから第2のオペレーティングシステムへ切り替える第1の切り替え命令により、第1のオペレーティングシステムから第2のオペレーティングシステムに切り替え、第2のオペレーティングシステムに対応する第2の仮想メモリ空間の論理アドレスN+1にあらかじめ記憶されたデータ取得命令、または、該論理アドレスN+1にあらかじめ記憶された命令以降に実行されるデータ取得命令を実行して、所定のレジスタから通信対象となるデータを取得することとしたので、従来の基盤OSやVMモニタ等の共通部分が不要で、第1および第2のオペレーティングシステムが共存され、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができるという効果を奏する。

【0204】

また、本発明によれば、第2のオペレーティングシステムは、データ取得命令を実行した後、あらかじめ仮想記憶された第2のオペレーティングシステムから第1のオペレーティングシステムへ切り替えるための第2の切り替え命令により、第2のオペレーティングシステムから第1のオペレーティングシステムに切り替えることとしたので、高いセキュリティと信頼性を維持したまま、オペレーティングシステムの切り替えおよび切り戻しを円滑におこなうことができるという効果を奏する。

【0205】

また、本発明によれば、所定のレジスタに格納されているデータをバックアップし、データがバックアップされたレジスタに通信対象となるデータを格納し、第2の切り替え命令により、第2のオペレーティングシステムから第1のオペレーティングシステムに切り替えがおこなわれた際に、バックアップされたデータをデータが格納されていた所定のレジスタに復元することとしたので、第1のオペレーティングシステムの実行中に使用されているレジスタにオペレーティングシステム間で通信するデータを格納することができ、そのレジスタを利用して通信をおこなうことにより、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができるという効果を奏する。

【0206】

また、本発明によれば、所定のレジスタは、第1のオペレーティングシステムの実行中に第1のオペレーティングシステムにより使用されていないレジスタであることとしたので、オペレーティングシステム間で通信するデータを格納することができ、そのレジスタを利用して通信をおこなうことにより、マルチオペレーティングシステムのセキュリティ、

10

20

30

40

50

信頼性を向上させることができるという効果を奏する。

【0207】

また、本発明によれば、所定のレジスタは、第1のオペレーティングシステムの実行中に第1のオペレーティングシステムにより使用されていないデバッグレジスタおよび／または汎用レジスタであることとしたので、デバッグレジスタおよび／または汎用レジスタにオペレーティングシステム間で通信するデータを格納することができ、そのレジスタを利用して通信をおこなうことにより、マルチオペレーティングシステムのセキュリティ、信頼性を向上させることができるという効果を奏する。

【0208】

また、本発明によれば、通信対象となるデータのサイズが所定のレジスタに格納できるサイズかどうかを判定し、格納できる場合には所定のレジスタにデータを格納し、格納できない場合には、所定のレジスタ以外の格納手段により通信対象となるデータを格納し、格納されたデータを第2のオペレーティングシステムが取得することとしたので、データのサイズに応じて適切な格納手段を選択することができ、高いセキュリティおよび信頼性を有する効率的なオペレーティングシステム間のデータの通信をおこなうことができるという効果を奏する。

【0209】

また、本発明によれば、ネットワークインターフェースカードに備えられた格納手段に第2のオペレーティングシステム宛の前記通信対象となるデータが格納された場合に、格納手段の接続を、第1のオペレーティングシステムを中継して第2のオペレーティングシステムに設定することとしたので、通信対象となるデータのサイズが所定のレジスタに格納できないサイズであっても、高いセキュリティおよび信頼性を有する効率的なオペレーティングシステム間のデータの通信をおこなうことができるという効果を奏する。

【0210】

また、本発明によれば、上記発明のいずれか一つに記載されたマルチオペレーティングシステム制御方法をコンピュータに実行させるようにしたので、プログラムがコンピュータ読み取り可能となり、これによって、上記発明のいずれか一つの動作をコンピュータによって実行することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明に係る実施の形態1の概略構成を示すブロック図である。

【図2】実施の形態1の具体的構成を示すブロック図である。

【図3】実施の形態1におけるマルチオペレーティングシステム間のメモリマッピングを説明する図である。

【図4】実施の形態1の動作原理を説明する図である。

【図5】実施の形態1の動作原理を説明する図である。

【図6】実施の形態1の動作例を説明する図である。

【図7】実施の形態1の動作例を説明するフローチャートである。

【図8】実施の形態1の動作例を説明するフローチャートである。

【図9】本発明に係る実施の形態2の構成を示すブロック図である。

【図10】実施の形態2の動作例を説明するブロック図である。

【図11】実施の形態2の動作例を説明するフローチャートである。

【図12】実施の形態2の動作例を説明するフローチャートである。

【図13】本発明に係る実施の形態1または2の応用例1～4を説明する図である。

【図14】実施の形態1または2をシステム移行に適用した場合を説明する図である。

【図15】実施の形態1または2を高セキュリティゲートウェイに適用した場合を説明する図である。

【図16】実施の形態1または2をデスクトップGrid端末に適用した場合を説明する図である。

【図17】実施の形態1または2を遠隔管理端末に適用した場合を説明する図である。

【図18】実施の形態1または2を高効率ネットサービス提供端末に適用した場合を説明

10

20

30

40

50

する図である。

【図 1 9】実施の形態 1 または 2 を高セキュリティ W e b サービス提供サーバに適用した場合を説明する図である。

【図 2 0】実施の形態 1 または 2 の変形例の構成を示すブロック図である。

【図 2 1】従来のマルチオペレーティングシステムの構成例 1 を示すブロック図である。

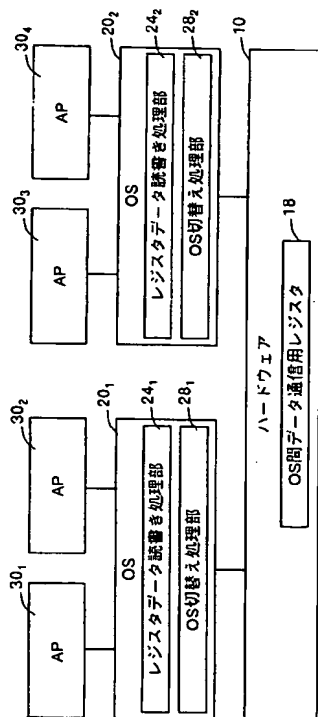
【図 2 2】従来のマルチオペレーティングシステムの構成例 2 を示すブロック図である。

【符号の説明】

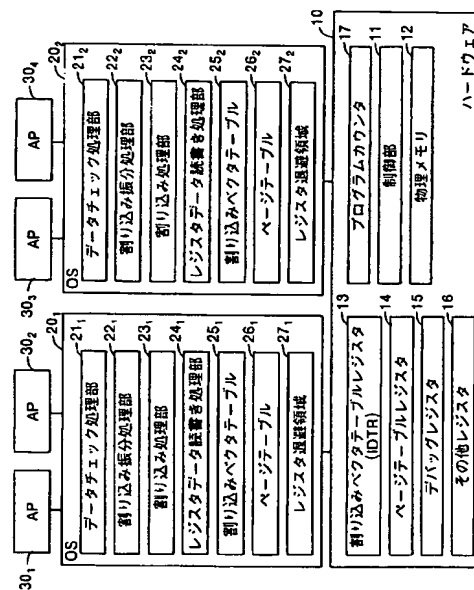
1 0	ハードウェア	
1 1	制御部	
1 2	物理メモリ	10
1 2 a ₁	, 1 2 a ₂	O S 用物理メモリ領域
1 2 b ₁	, 1 2 b ₂	A P 用物理メモリ領域
1 3	割り込みベクタテーブルレジスタ	
1 4	ページテーブルレジスタ	
1 5	デバッグレジスタ	
1 6	その他のレジスタ	
1 7	プログラムカウンタ	
1 8	O S 間データ通信用レジスタ	
2 0 ₁	, 2 0 ₂	O S
2 1 ₁	, 2 1 ₂	データチェック処理部
2 2 ₁	, 2 2 ₂	割り込み振り分け処理部
2 3 ₁	, 2 3 ₂	割り込み処理部
2 4 ₁	, 2 4 ₂	レジスタデータ読書き処理部
2 5 ₁	, 2 5 ₂	割り込みベクタテーブル
2 6 ₁	, 2 6 ₂	ページテーブル
2 7 ₁	, 2 7 ₂	レジスタ退避領域
2 8 ₁	, 2 8 ₂	O S 切り替え処理部
2 9 ₁	, 2 9 ₂	データサイズ判定部
3 0 ₁	, 3 0 ₂	A P
4 0 ₁	, 4 0 ₂	仮想メモリ空間
4 0 a ₁	, 4 0 a ₂	O S 用仮想メモリ空間
4 0 b ₁	, 4 0 b ₂	A P 用仮想メモリ空間
5 0	ネットワーク	
6 0	N I C	
6 1	N I C 送信処理部	
6 2	送信バッファ	
6 3	N I C 受信処理部	
6 4	受信バッファ	
6 5	受信バッファレジスタ	
6 6	送信バッファレジスタ	40
7 0 ₁	, 7 0 ₂	N I C デバイスドライバ
7 1 ₁	, 7 1 ₂	送信処理部
7 2 ₁	, 7 2 ₂	送信バッファ
7 3 ₁	, 7 3 ₂	受信処理部
7 4 ₁	, 7 4 ₂	受信バッファ
1 0 0	コンピュータ	
1 1 0	C P U	
1 2 0	入力装置	
1 3 0	R O M	
1 4 0	R A M	50

- 150 読取装置
160 出力装置
170 バス
200 記録媒体

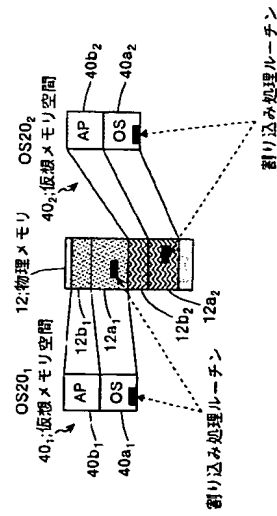
【図1】



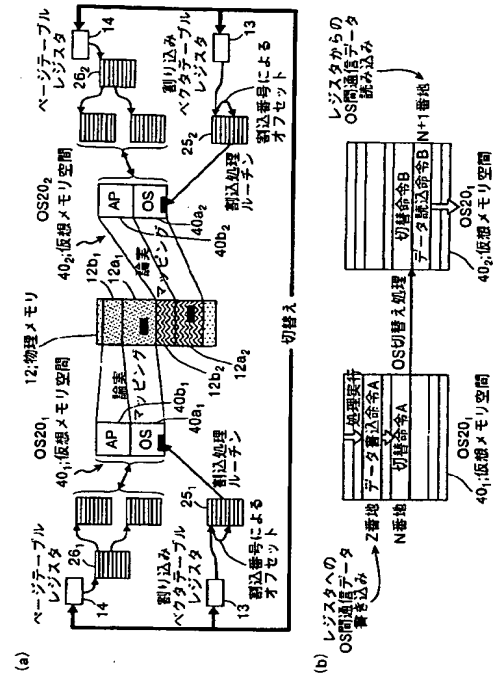
【図2】



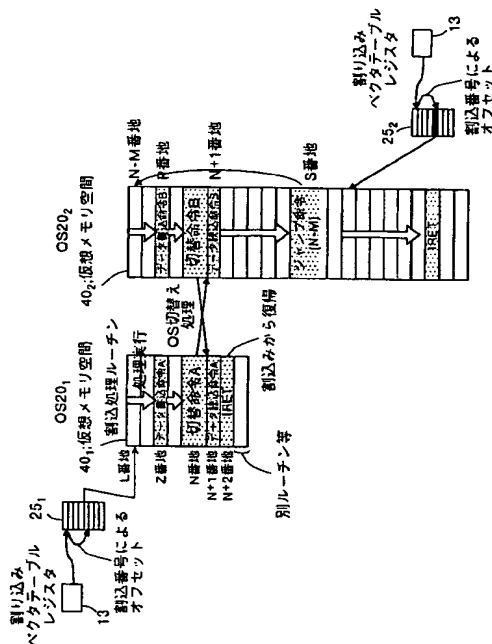
【図 3】



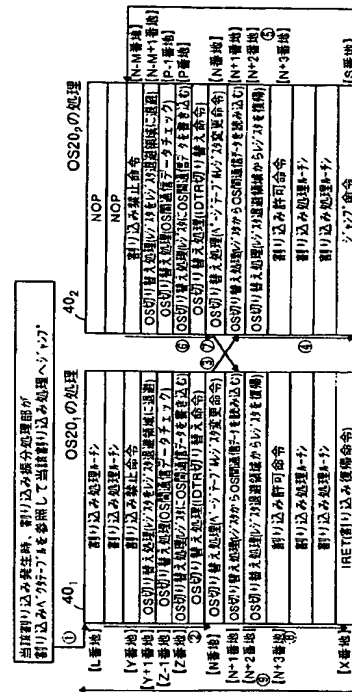
【図 4】



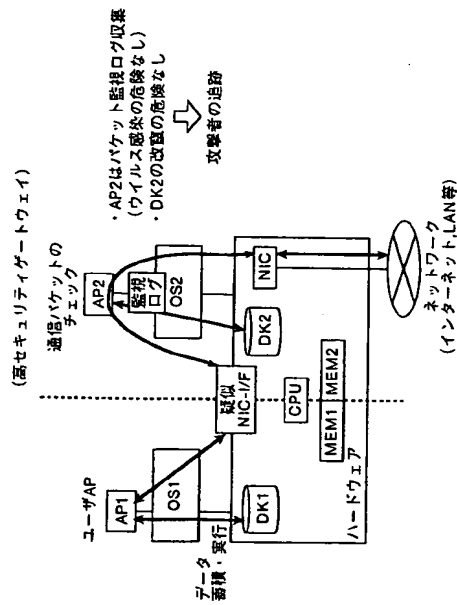
【図 5】



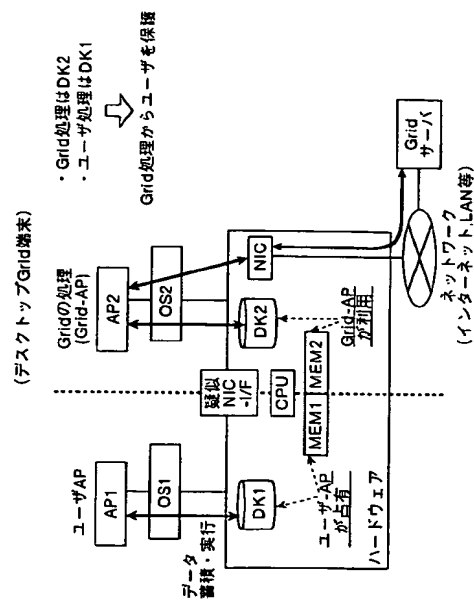
【図 6】



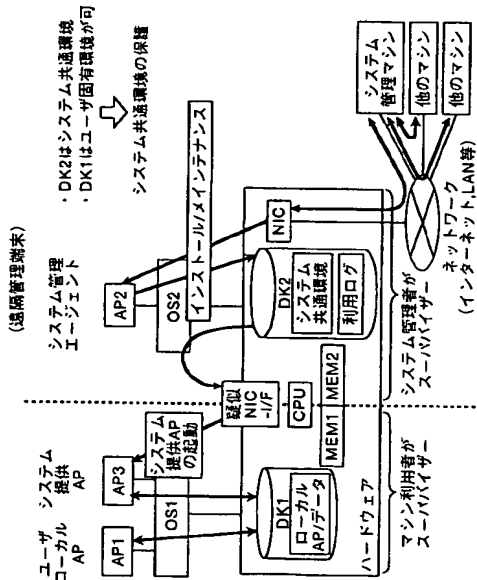
【図 15】



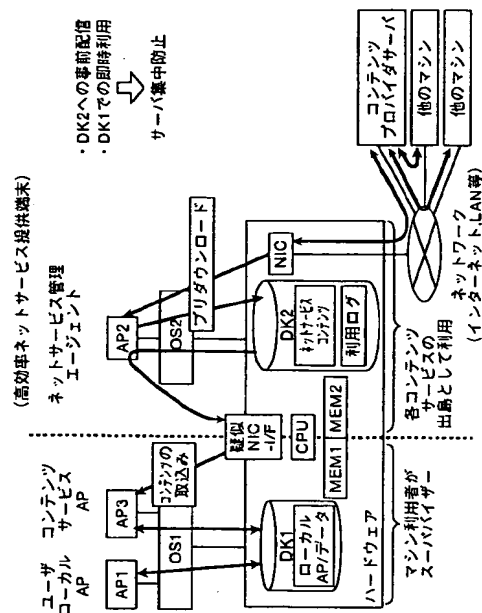
【図 16】



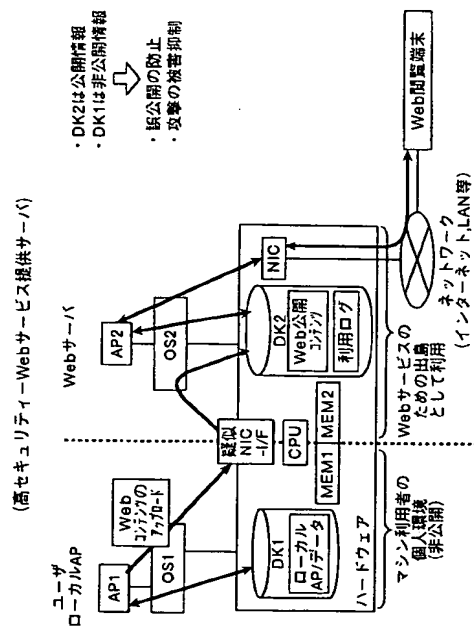
【図 17】



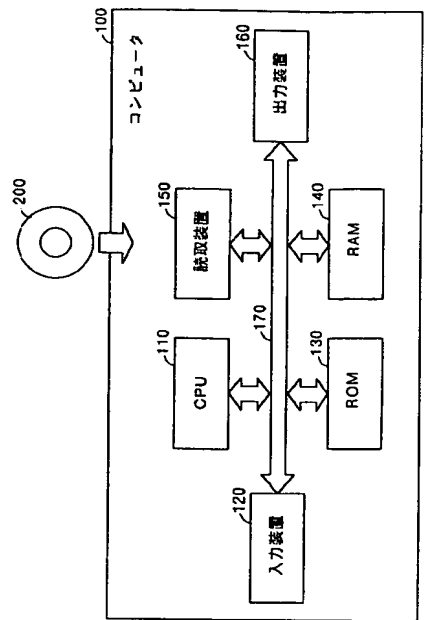
【図 18】



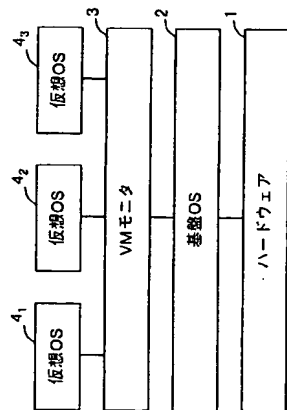
【図 19】



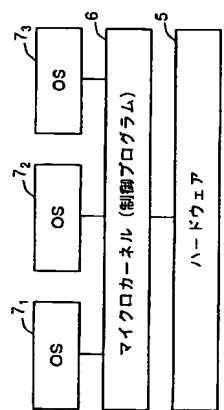
【図 20】



【図 21】



【図 22】



フロントページの続き

- (72)発明者 伊藤 健一
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内
- (72)発明者 中島 雄作
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内
- (72)発明者 田淵 正樹
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内
- (72)発明者 榎本 圭
東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内
- Fターム(参考) 5B098 HH01 HH04

